

# Smartphone data safety with quantum cryptography

January 20, 2012



## New technology brings quantum cryptography to handhelds

*Laws of quantum physics and information theory ensure that smartphones with QKarD could never be compromised*

The Quantum Smart Card, developed by LANL researchers, that loads quantum cryptography onto a smartcard or smart phone, creates an impenetrable line of defense.

QKarD, a patent-pending technology and the culmination of 18 years of research at LANL, uses a new type of symmetric key distribution, known as quantum cryptography or quantum key distribution, which is based on the quantum mechanical laws of physics. The technology has many advantages over other key distribution methods. The laws of quantum physics and information theory ensure that these keys never can be cracked, regardless of advancements in computer technology.

## **Higher security, lower computational requirements**

To encrypt and decrypt messages, cryptographic algorithms require that the sender and receiver each have the same secret keys to determine how their cryptographic functions operate mathematically.

The asymmetric key delivery that is commonly used today is based on difficult mathematical problems. Its security cannot be guaranteed, and it can be difficult for a small device to perform the required mathematics. Quantum key distribution uses polarized single photons to generate and distribute secret keys with higher security and much lower computational requirements.

## **QKarD could fit into smartphones**

Current quantum key distribution systems are bulky, rack-mounted systems requiring dedicated fiber optic lines to connect users within limited distances. Second lines carry other optical signals needed for the protocol information and the secured data.

QKarD does not require a second line, and it minimizes the technology to fit into smaller devices, such as a smartphone. QKarD can be used whether the device is plugged into a charging/docking station or is mobile.

## **Random cryptographic keys encode, decode information**

The miniature transmitter communicates with a trusted authority to generate random cryptographic keys to encode and decode information. To make a secure phone call on a smartphone, User A would first be authenticated with a password and perhaps biometric readings.

User A would then dial the number of User B, a person with a QKarD. If User B is in User A's nonsecret lookup table, the QKarD uses its secret keys to set up a secure call. If User B's information is not in User A's lookup table, the QKarD calls the trusted authority via a normal cellular call and uses a QKarD key to encrypt the key that the trusted authority will apply to the phone call.

## **QKarD could replace current security systems**

Available for licensing from the Technology Transfer Division, QKarD could replace current security systems for banking, online transactions, access to secure facilities, border crossings, digital rights management controls, and electronic voting. It is simpler and more affordable than other systems.

